IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method of securing digital content on a hard drive of a computer, comprising: [detecting] providing a [portable,] physical key adapted to be carried by a user; detecting the [portable,] physical key with a receiver/decoder circuit [associated] communicating with the hard drive;
validating the detected physical key with the receiver/decoder circuit wherein validating includes determining whether or not the detected physical key is associated with the hard drive; and
permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected key is validated wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the detected physical key in order to provide sector-level protection.

2. (Original) The method of claim 1, wherein the receiver/decoder circuit resides in the computer.

3. (Original) The method of claim 1, wherein the detecting step includes detecting the key over a secure wireless link.

4. (Canceled) The method of claim 1, wherein the validating step includes determining whether or not the detected key is associated with the hard drive.

5. (Currently Amended) The method of claim [4] 1, wherein the receiver/decoder circuit enables the hard drive if the detected key is validated and disables the hard drive if the detected key is not validated in order to provide hard drive level protection.

6. (Currently Amended) The method of claim 5, wherein digital content stored on the [computer] drive is not encrypted with the key.

7. (Canceled) The method of claim 4, wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the key associated with the hard drive in order to provide sector-level protection.

8. (Currently Amended) The method of claim [4] 1, wherein the key associated with the hard drive is initially delivered with the hard drive.

9. (Currently Amended) A system for securing digital content on a hard drive of a computer, comprising:

a [portable,] physical key adapted to be carried by a user;

a hard drive having digital content; and

a receiver/decoder circuit communicating with the hard drive for detecting and validating the physical key wherein the receiver/decoder circuit validates the physical key by determining whether or not the detected physical key is associated with the hard drive wherein the receiver/decoder circuit decrypts or encrypts digital content read from or written to the hard drive using the physical key associated with the hard drive in order to provide sector-level protection. [and for permitting access to the hard drive or a portion thereof if the detected key is valid, the receiver/decoder circuit being associated with the hard drive].

10. (Original) The system of claim 9, wherein the receiver/decoder circuit resides in the computer.

11. (Original) The system of claim 9, wherein the receiver/decoder circuit detects the key over a secure wireless link.

12. (Canceled) The system of claim 9, wherein the receiver/decoder circuit validates the key by determining whether or not the detected key is associated with the hard drive.

13. (Currently Amended) The system of claim [12] 9, wherein the receiver/decoder circuit enables the hard drive if the detected physical key is validated and disables the hard drive if the detected key is not validated in order to provide hard drive level protection.

14. (Currently Amended) The system of claim[13] 9, wherein digital content stored on the computer is not encrypted with the physical key.

15. (Canceled) The system of claim 12, wherein the receiver/decoder circuit decrypts or encrypts digital content read from or written to the hard drive using the key associated with the hard drive in order to provide sector-level protection.

16. (Currently Amended) The system of claim [12] 9, wherein the physical key associated with the hard drive is initially delivered with the hard drive.

17. (Canceled) A method of securing and accessing a computer file, comprising: encrypting the file with a receiver/decoder circuit using a portable, physical key; storing the encrypted file on a storage medium; requesting the file with a playback mechanism; detecting the key with the receiver/decoder circuit; validating the detected key with the receiver/decoder circuit; and if the detected key is validated, decrypting the file with the receiver/decoder circuit using the detected key, whereby the decrypted file can be played back with the playback mechanism.

18. (Canceled) The method of claim 17, wherein the storage medium is a hard drive of a computer, and the receiver/decoder circuit resides in the computer.

19. (Canceled) The method of claim 17, wherein a software driver in the computer's operating system instructs the receiver/decoder circuit to perform the detecting, validating, and decrypting steps.

20. (Canceled) The method of claim 17, wherein the detecting step includes detecting the key over a secure wireless link.

21. (Canceled) The method of claim 17, wherein the validating step includes determining whether or not the detected key is associated with the file.

22. (Canceled) A system for securing a computer file and later accessing the file for playback by a playback mechanism, the system comprising: a portable, physical key; a receiver/decoder circuit for using the key to encrypt the file; and a storage medium for storing the encrypted file; the receiver/decoder circuit for detecting and validating the key and, if the detected key is validated, using the key to decrypt the encrypted file, whereby the decrypted file can be played back with the playback mechanism.

23. (Canceled) The system of claim 22, wherein the storage medium is a hard drive of a computer, and the receiver/decoder circuit resides in the computer.

24. (Canceled) The system of claim 22, wherein a software driver in the computer's operating system instructs the receiver/decoder circuit to detect and validate the key and to use the key to decrypt the file.

25. (Canceled) The system of claim 22, wherein the receiver/decoder circuit detects the key over a secure wireless link.

Please add the following new claims:

26. (New) The method of claim 1 wherein each sector is encrypted or decrypted by receiver/decoder circuit using the personal digital key associated with a drive corresponding to the sector.

27. (New) The method of claim 1 wherein the sector level protection includes individual data sectors and clusters of data sectors.

28. (New) A method of securing a hard drive of a computer, comprising:

providing a portable, physical key adapted to be carried by a user;

wirelessly detecting the portable, physical key with a receiver/decoder circuit communicating with the hard drive when the key is in proximity to the receiver/decoder circuit;

validating the detected portable physical key with the receiver/decoder circuit; and

permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected portable physical key is validated.

29. (New) The method of claim 28 wherein the receiver/decoder circuit enables the hard drive if the detected key is validated and disables the hard drive if the detected key is not validated in order to provide hard drive level protection.

30. (New) The method of claim 29 wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the key associated with the hard drive.

31. (New) A system of securing a hard drive of a computer, comprising: a portable, physical key adapted to be carried by a user; and, a receiver/decoder circuit; wherein when the receiver/decoder circuit wirelessly detects the portable physical key, the receiver/decoder circuit validates the portable physical key and permits access to the hard drive or a portion thereof.